CLAIMS

What is claimed is:

1. A computer-implemented method for configuring and scheduling a security audit of a computer network comprising the steps of:

conducting a discovery scan to identify an element of the computer network and determine the element's functions;

configuring an audit scan to perform on the element, wherein the audit scan is a more thorough scan than the discovery scan;

scheduling a time to perform the audit scan on the element;

running the audit scan of the element at the scheduled time;

calculating a security score for the element based on the audit scan; and

scheduling another time to repeat the audit scan on the element, the scheduling based on the results of the audit scan.

2. The method of Claim 1, further comprising the step of configuring a subsequent audit scan of the element that is different from the audit scan.

3. The method of Claim 1, further comprising the step of receiving a blackout time during which no audit scan can be scheduled.

4. The method of Claim 1, wherein the step of conducting a discovery scan further comprises identifying the function of the element.

5. The method of Claim 1, wherein the step of conducting a discovery scan further comprises identifying vulnerabilities associated with the element.

6. The method of Claim 1, wherein the step of conducting a discovery scan further comprises assigning an asset value for the element, wherein the asset value indicates the relative importance of the element in the network.

7. The method of Claim 6, wherein the asset value is modified based on the audit scan.

8. The method of Claim 1, further comprising the step of receiving a manually selected asset value for the element.

9. The method of Claim 1, wherein the step of configuring an audit scan comprises selecting a type of audit scan based on the discovery scan.

10. The method of Claim 1, wherein the step of configuring an audit scan comprises:

retrieving an asset value based on the discovery scan;

retrieving a scan frequency associated with the asset value, wherein the scan frequency indicates how often the scan is performed; and

assigning a role based on the discovery scan, wherein the role indicates the function of the element; and

assigning a policy based on the discovery scan, wherein the policy indicates the type of audit scan.

11. The method of Claim 1, wherein the step of configuring an audit scan comprises manually selecting the type of audit scan.

12. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

13. A computer-implemented method for configuring and scheduling a security audit of a computer network comprising the steps of:

conducting a discovery scan to identify an element of the computer network;

configuring an audit scan to perform on the element;

scheduling a time to perform the audit scan on the element; and

running the audit scan at the scheduled time on the element.

14. The method of Claim 13, further comprising the step of calculating a security score for the element based on the audit scan.

15. The method of Claim 13, further comprising the step of scheduling another time to perform the audit scan on the element.

16. The method of Claim 13, further comprising the step of receiving a blackout time during which no audit scan can be scheduled.

17. The method of Claim 13, wherein the step of conducting a discovery scan further comprises identifying at least one of the functions or vulnerabilities associated with the element.

18. The method of Claim 13, wherein the step of conducting a discovery scan further comprises assigning an asset value for the element.

19. The method of Claim 13, wherein the step of configuring an audit scan comprises:

retrieving an asset value based on the discovery scan;

retrieving a scan frequency associated with the asset value; and

assigning a role and a policy based on the discovery scan.

20. The method of Claim 13, wherein the step of configuring an audit scan comprises manually selecting the type of audit scan.

21. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 1.

22. A method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element and the function of the network element;

selecting an audit scan to perform on the network element, the selection based on the initial scan, wherein the audit scan is more thorough than the initial scan;

scheduling the audit scan to perform on the network element;

performing the audit scan on the network element at the scheduled time;

receiving data from the selected audit scan of the network element; and

computing a security score for the network element from the selected audit scan.

23. The method of Claim 22, further comprising modifying the selected audit scan; said modification based on the data received from the selected audit scan.

24. The method of Claim 22, wherein the step of receiving an initial scan comprises:

identifying an operating system for the network element;

identifying a service for the network element, the service indicating the element's function;

determining an asset value of the network element from the operating system and the service of the network element, the asset value indicating the relative importance of the network element; and

identifying a vulnerability associated with the network element.

25. The method of Claim 22, wherein the step of selecting an audit scan is based on the initial scan.

26. The method of Claim 22, wherein the step of selecting an audit scan is based on a manual input.

27. The method of Claim 22, wherein the step of scheduling the audit scan comprises checking a blackout schedule.

28. The method of Claim 22, wherein the step of computing a security score comprises summing one or more vulnerabilities associated with the element.

29. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 22.

30. A method for assessing the security of a network comprising the steps of:

receiving an initial scan identifying a network element;

selecting an audit scan to perform on the network element, said selection based on the initial scan;

performing the selected audit scan on the network;

receiving data from the selected audit scan of the network element; and

computing a security score for the network element from the selected audit scan.

31. The method of Claim 30, further comprising the step of scheduling the selected audit scan, said scheduling based on the initial scan.

32. The method of Claim 30, further comprising modifying the selected audit scan, said modification based on the data received from the selected audit scan.

33. The method of Claim 30, wherein the step of receiving an initial scan comprises:

identifying an operating system and a service for the network element;

determining an asset value of the network element from the operating system and the service of the network element; and

identifying a vulnerability associated with the network element.

34. The method of Claim 30, wherein the step of selecting an audit scan is based on the initial scan.

35. The method of Claim 30, wherein the step of selecting an audit scan is based on a manual input.

36. The method of Claim 30, wherein the step of scheduling the audit scan comprises checking a blackout schedule.

37. The method of Claim 30, wherein the step of computing a security score comprises summing one or more vulnerabilities associated with the element.

38. A computer-readable medium having computer-executable instructions for performing the steps recited in Claim 30.

39. A system for configuring and scheduling a security audit of a computer network comprising:

the computer network;

a security audit system operable for conducting a discovery scan to identify an element of the computer network and configuring and scheduling an audit scan of the element; and

a console operable for receiving information from the security audit system and transmitting information to the security audit system about the discovery scan and the audit scan.

40. The system of Claim 39, wherein the security audit system is further operable for conducting a discovery scan to:

identify a function for the element;

determine an asset value for the element; and

identify a vulnerability for the element.

41. The system of Claim 39, wherein the security audit system checks a blackout schedule before scheduling an audit scan.

42. The system of Claim 39, wherein the security audit system further comprises a system scanning engine operable for detecting particular vulnerabilities on the network element.

43. The system of Claim 39, wherein the security audit system further comprises an Internet scanning engine operable for performing a discovery scan on the network.

44. The system of Claim 39, wherein the security audit system further comprises a database scanning engine operable for detecting vulnerabilities in database elements within the network.

45. The system of Claim 39, wherein the security audit system further comprises an active scan engine operable for selecting, coordinating, and scheduling various discovery and audit scans to be performed on the computer network.